KASPERSKY lab

Protección avanzada e inteligente frente a amenazas para mitigar el riesgo de los ataques dirigidos

Kaspersky Threat Management and Defense Solution

www.kaspersky.es
#truecybersecurity

El riesgo creciente de amenazas avanzadas y ataques dirigidos

Crecimiento del 200 % del coste de recuperación iniciado el mismo día o tras la semana de la detección de una brecha de seguridad de las empresas*

*Resultados de la encuesta de riesgos de seguridad de IT empresarial de 2016 realizada en todo el mundo por Kaspersky Lab

El **15 %** de las empresas ha experimentado un ataque dirigido y más del 53 % de ellas ha perdido datos confidenciales debido a dichos ataques.*

*Informe de riesgos de seguridad de IT globales de 2015 de Kaspersky

Todas las empresas lo bastante grandes como para ocupar un lugar significativo en su mercado puede sufrir un ataque. Esto no significa que las más pequeñas sean inmunes; en muchos casos, los delincuentes las ven como un objetivo fácil a partir del que acceder al siguiente más grande. Pero cuando se trata de los líderes del mercado, las probabilidades de convertirse en víctima de un ataque de este tipo aumentan considerablemente. No es una cuestión de escenarios hipotéticos, sino de cuándo se producirán los ataques...

¿Quién ataca?

Cibercriminales, que venden datos al mejor postor o simplemente roban dinero. Suelen desarrollar sus propias herramientas virtuales o comprarlas en la web oscura.

Empresas de la competencia, que buscan datos confidenciales o incluso cometer sabotaje. Suelen contratar los servicios de cibermercenarios.

Cibermercenarios, maestros del ciberespionaje que desarrollan sus propias herramientas y venden sus "servicios" al mejor postor.

Hacktivistas, que sostienen trabajar por el bien común, son ingeniosos, usan herramientas complejas y presentan un grave problema para las organizaciones que despierten su interés

Agencias gubernamentales, que aunque lo nieguen, se sabe que los gobiernos del mundo hacen un seguimiento de las personas, grupos y empresas. Sus herramientas pueden ser muy sofisticadas, caras y difíciles de detectar.

Panorama de amenazas dirigidas a las grandes empresas

Los ataques dirigidos y las amenazas avanzadas, incluidas las amenazas persistentes avanzadas (APT), se encuentran entre los riesgos más peligrosos a los que se enfrentan los sistemas empresariales. Sin embargo, aunque las amenazas y las técnicas que utilizan los cibercriminales evolucionan constantemente, muchas organizaciones dependen de tecnologías de seguridad anticuadas y aplican planteamientos obsoletos para protegerse de las amenazas actuales y futuras.

Las amenazas avanzadas y especialmente dirigidas a las empresas pueden pasar inadvertidas durante semanas, meses o incluso años, mientras que sus actores recopilan lenta y silenciosamente información, y trabajan para explotar las vulnerabilidades específicas de los sistemas que han elegido para sus ataques. Al contrario que el malware común, los autores de las amenazas dirigidas avanzadas pueden controlarlas activamente. El objetivo no se limita a la propagación de malware, sino penetrar en el perímetro empresarial. Estos ataques suelen ser el resultado de una investigación paciente y meticulosa de sus creadores, que saben esperar animados por la expectativa de conseguir sus objetivos.

Pérdida media causada por un solo ataque dirigido:

Factores internos y externos que propician el éxito de los ataques

Entre los principales factores que propician la culminación satisfactoria de los ataques dirigidos a las infraestructuras de IT se incluyen:

- IT oculta y en la clandestinidad
- Conectividad incontrolada de dispositivos de IoT
- Excesiva dependencia de la digitalización
- Falta de capacidades preventivas y optimismo excesivo en las garantías de seguridad del perímetro actual
- Escaso conocimiento de los riesgos para la seguridad de la información por parte de los empleados
- Falta de visibilidad del entorno de IT y en concreto del enrutamiento de las redes
- Sistemas operativos, y software desfasados y con tecnología propietaria
- Falta de cualificación de los miembros del equipo de seguridad en materia de investigación del malware, ciencia forense digital, respuesta a incidentes e inteligencia frente a amenazas

¿Qué es el riesgo?

Riesgos para todas las organizaciones:

- Transacciones no autorizadas
- Robo o daños de datos críticos
- Manipulación invisible de procesos
- Reducción de la capacidad de la competencia
- Chantaje y extorsión
- Robo de identidad

Riesgos para sectores industriales clave:

Servicios financieros

- Transacciones no autorizadas
- Ataques a cajeros con robo físico de efectivo
- Robo de identidad

Gubernamental

- Manipulación de datos
- Espionaje
- Disponibilidad limitada de los servicios en línea
- Robo de identidad
- Actos de hacktivismo

Fabricación y alta tecnología

- Espionaje (procedimientos)
- Procesos tecnológicos críticos comprometidos

Telecomunicaciones

- Ataque a clientes corporativos con infraestructura de telecomunicaciones
- Manipulación de servidores de correo para ingeniería social
- Control de facturación
- Manipulación de recursos web para fines de phishing
- Uso de infraestructura comprometida (dispositivos/IoT) para ataques DDoS

Energía y servicios públicos

- Manipulación de datos de cálculos
- Ataques a las redes tecnológicas con daños físicos

Medios de comunicación

- Activismo de hackers
- Sitio web atacado (destrucción o phishing) y propagación de ataques entre el público masivo

Asistencia sanitaria

- Robo de información de pacientes
- Ataques a equipos de telemedicina

Ataques dirigidos: el cibercrimen como profesión

La mayoría de los ataques dirigidos son supervisados por cibercriminales y hackers avezados que saben cómo adaptar cada fase para sortear las defensas tradicionales, explotar las carencias y maximizar la cantidad de activos valiosos que pueden hurtar, incluido dinero y datos confidenciales.

Los hackers del pasado se han metamorfoseado en profesionales para los que el cibercrimen es un negocio. La única motivación de sus ataques a una empresa es sacar el máximo provecho, para lo cual calculan todo antes de lanzarlos y cotejan los costes asociados y las recompensas posibles. Por supuesto, el objetivo es minimizar los costes iniciales abaratando los ataques todo lo posible, con máximos resultados económicos.

La mayoría de los ataques dirigidos combinan ingeniería social y una serie de herramientas personalizadas. El coste de lanzar un ataque dirigido eficaz se ha reducido de forma notable, con un aumento proporcional en el número total de ataques globales.

Por tanto, ¿a qué riesgos se enfrenta cuando una organización como la suya cae víctima de un ataque dirigido?

Daño directo	Gasto reactivo
 Corrección +  Pérdida de oportunidades +  Inactividad	 Sistemas +  Personal +  Formación
	Para evitar nuevas infracciones

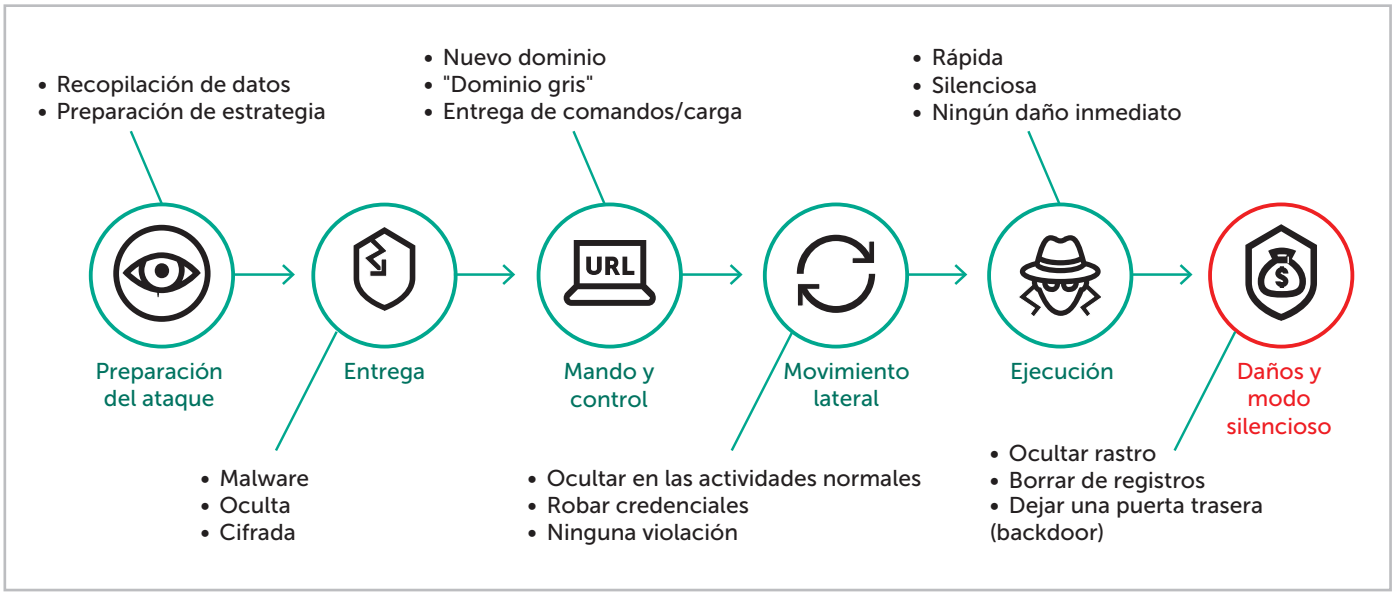
Pérdidas económicas directas Los atacantes pueden cometer ciberfraudes robando credenciales bancarias para acceder a las cuentas corporativas y realizar transacciones fraudulentas.

Interrupción de los procesos empresariales. Algunos ataques son meros subproductos y solo alteran o ralentizan procesos empresariales críticos; en cambio, el objetivo de otros es un sabotaje completo. Incluso si el ataque es detectado, es probable que transcurra cierto tiempo hasta que la empresa afectada realice las investigaciones oportunas y recupere sus operaciones, y en este ínterin podrían perderse aún más oportunidades de negocio.

Costes de la limpieza Tras un ataque, puede que se vea obligado a sufragar toda una serie costes imprevistos. Para la recuperación de los sistemas y procesos, es probable que deba afrontar gastos operativos y de capital, por ejemplo, por la contratación de consultores de sistemas y seguridad.

Anatomía de un ataque dirigido

En teoría, la cadena de un ataque dirigido parece bastante sencilla y directa: reconocimiento y prueba, penetración, propagación, ejecución, resultados. Esta cadena podría sugerir que si se bloquean automáticamente los primeros pasos de un ataque de varias fases, el ataque en sí quedaría frustrado.



Pero la realidad es que los ataques dirigidos son muy sofisticados y no lineales en términos de progresión y ejecución. Por tanto, una estrategia de defensa de varios niveles debe incluir capacidades de detección automatizadas, supervisión continua y búsqueda de amenazas.

Los ataques dirigidos son procesos a largo plazo que ponen en riesgo la seguridad y brindan al atacante el control de la infraestructura de IT de la víctima, sin su autorización. Además, ayudan al atacante a evitar la detección mediante tecnologías de seguridad tradicionales.

Aunque algunos ataques pueden utilizar las amenazas persistentes avanzadas (APT), que pueden ser muy eficaces pero caras de implementar, otros ataques pueden utilizar una sola técnica, como malware avanzado o un exploit de día cero.

Un ataque dirigido es un proceso prolongado que elude la seguridad y permite a un cibercriminal obviar los procedimientos de autorización e interactuar con la infraestructura de IT, para evitar así la detección con los medios tradicionales.

Por tanto y en primer lugar, es un proceso, una actividad continuada en el tiempo, un proyecto, y no una acción maliciosa aislada. Por nuestra experiencia en la supervisión de ataques globales, estos procesos suelen prolongarse al menos 100 días, y en el caso de organismos gubernamentales, grandes actores del mercado e infraestructuras críticas, los tiempos pueden calcularse en años.

En segundo lugar, el proceso se dirige a una infraestructura específica, se diseña para superar determinados mecanismos de seguridad y podría apuntar inicialmente a los empleados a través del correo electrónico o la red social. Esta metodología es muy distinta a la de los correos masivos de los atacantes que emplean software malicioso estándar y que operan con unos objetivos totalmente diferentes. En el caso de los ataques dirigidos, la metodología y las fases de la cadena de ataque se establecen en función de la víctima específica.

En tercer lugar, esta operación suele ser gestionada por un grupo organizado o un equipo de profesionales, a veces de carácter internacional, dotados de sofisticadas herramientas técnicas. Bien podría decirse que sus actividades no se circunscriben solo a un proyecto, sino que se integran en una operación multicombate. Por ejemplo, los atacantes suelen compilar una lista de empleados susceptibles de convertirse en la "vía de acceso" a las redes y organización objetivo, y estudian sus perfiles online y actividad en las redes sociales. Seguidamente, la tarea de hacerse con el control del equipo de trabajo de la víctima queda virtualmente solucionada. El equipo del empleado queda infectado y los intrusos continúan su avance para hacerse con el control de la red, desde donde pueden dirigir sus actividades delictivas.

Desafíos de seguridad empresarial

El crecimiento exponencial de las amenazas sofisticadas está llevando a muchas empresas a implementar tecnologías y servicios con la esperanza de aumentar la visibilidad y la protección frente a las amenazas actuales. Pero sin un enfoque multidisciplinar y una planificación estratégica, estos esfuerzos pueden no colmar todas las expectativas.

Entre los resultados decepcionantes de una inversión en seguridad no estructurada o irregular se encuentran:

1. Inversión importante en un sandbox, en tecnologías independientes o en la creación de un SOC, que finalmente no generan mejoras proporcionales en los resultados para la seguridad.

Las técnicas de seguridad perimetrales, como firewalls y software antimalware pueden frenar algunos de los ataques más oportunistas. Pero los ataques dirigidos son harina de otro costal.

Algunos proveedores han pensado combatir las APT con varios productos independientes: sandbox, análisis de anomalías en la red o incluso supervisión centrada en los endpoints. Si bien estos elementos individuales pueden y, de hecho, ofrecen cierta protección contra las herramientas de los cibercriminales, no son suficientes por sí solos para detectar un ataque dirigido coordinado.

Para ello, se requiere la detección de varios eventos desencadenados en todos los niveles de la infraestructura empresarial. A continuación, la información obtenida puede procesarse con un sistema de análisis de varios niveles, seguida de su interpretación aplicando inteligencia de seguridad en tiempo real procedente de una fuente de confianza. En otras palabras, lo mejor es invertir en un enfoque que incorpore lo mejor de muchas tecnologías, como sandbox con análisis de anomalías en la red y análisis de eventos de endpoints, en un proceso integral.

2. Las soluciones actuales generan demasiados eventos de seguridad como para que su equipo de SOC pueda procesar, analizar, controlar y responder a todos ellos en un plazo razonable.

3. Falta de competencias en seguridad acordes a los niveles actuales de sofisticación de las amenazas. Los expertos en seguridad pueden estar formados en la detección de incidentes y la corrección rápida (plantilla "oro", lista negra de URL/archivos, creación de algunas reglas), pero no totalmente cualificados para implementar un proceso de respuesta integral (clasificación de niveles de riesgo, realización de análisis iniciales, investigación, contención y análisis forenses)

4. Falta de visibilidad operativa En un ataque dirigido, los cibercriminales pueden evadir fácilmente las soluciones de seguridad tradicionales usando credenciales robadas y software legítimo, por lo que en apariencia no vulneran ningún sistema.

Como los atacantes hacen todo lo posible para ocultar sus actividades maliciosas, puede ser muy difícil para un equipo de seguridad de IT interno identificar un ataque, por lo que los atacantes pueden seguir ocasionando daños durante un largo periodo de tiempo.

La realidad es que el malware es responsable de solo el 40 % de las infracciones. Según hemos podido comprobar, los actores de las amenazas usan diversas técnicas para acceder a los sistemas de las empresas.Incluso si se usa malware, entre el 70 y el 90 % es exclusivo de la organización en la que se detecta (Verizon: Data Breach Investigation Report [Informe de investigación de robo de datos]).

5. La dificultad asociada a determinar qué conocimientos aplicar y desarrollar internamente, qué tarea de seguridad subcontratar y qué puede delegar en los sistemas automatizados.

Dada la creciente gravedad de los incidentes de seguridad y su impacto potencial en la eficiencia general de las empresas, uno de los principales desafíos a los que se enfrentan los departamentos de seguridad es rodearse de un buen equipo de expertos cualificados con las competencias adecuadas. Una estrategia de seguridad totalmente eficaz requiere de capacidades de detección y supervisión continuas, además de una respuesta rápida y una corrección adecuada, con procesos de análisis forenses relevantes.

Los equipos de SOC convencionales suelen centrarse solo en parte de esta tarea: la detección y respuesta. La implementación de soluciones automatizadas permite a los expertos dedicarse a los siguientes pasos del proceso de gestión de incidentes, pero son pocas las empresas preparadas para llevar a cabo internamente las distintas tareas de alto nivel. Por tanto, el desafío consiste en identificar qué elementos de todo el proceso (gestión, clasificación del riesgo, priorización o recuperación rápida) deben asignarse al equipo interno y cuáles (investigación del malware, ciencia forense digital, respuesta al incidente o búsqueda de amenazas) se completarán más eficazmente externalizándolos en especialistas competentes.

Acerca de los sandbox

Muchas de las soluciones de detección de ataques dirigidos del mercado solo constan de un sandbox independiente. Incluso los proveedores sin registro de detección de amenazas nuevas ni avanzadas afirman ofrecer sandboxes que a menudo no son más que una extensión de sus motores antimalware y no proporcionan ninguna inteligencia sobre amenazas.

El sandbox avanzado de Kaspersky Lab es solo una parte más de nuestras capacidades de detección integradas. Se ha desarrollado directamente a partir de nuestro complejo sandbox de laboratorio, la tecnología que llevamos más de una década usando. Sus capacidades se han mejorado con las estadísticas recopiladas tras diez años de análisis de amenazas, por lo que es una solución más madura y mejor orientada a las amenazas dirigidas que las milagrosas soluciones sandbox actualmente en oferta.

El SOC de empresa basado en la inteligencia

Los cibercriminales han adaptado sus técnicas para eludir las defensas tradicionales y acechan sin ser detectados en sistemas durante meses o incluso años. Ha llegado el momento de que la seguridad empresarial se adapte a esa situación con un enfoque inteligente a varios niveles en términos de seguridad de IT.

Hasta hace poco, bastaba con defender el perímetro corporativo usando tecnologías de seguridad comunes que evitaban infecciones de malware o acceso no autorizado a la red corporativa. Sin embargo, actualmente, con el aumento de ataques dirigidos, este enfoque sencillo ya no sirve.

Si su departamento de seguridad desea levantar barreras de protección contra peligros nuevos, necesita un enfoque altamente adaptable de varios niveles basado en un SOC convencional dotado de inteligencia sobre amenazas y soluciones de seguridad de multicapa.

Mejora de los procesos de seguridad empresarial

El departamento de seguridad de la información es responsable de la protección técnica y organizativa de la información crítica y de los procesos empresariales en entornos de IT con frecuencia complejos. Esto incluye, por ejemplo, la creciente adopción de soluciones automatizadas y componentes de software, y la transición hacia la gestión de documentos electrónicos.

La avalancha de amenazas avanzadas y ataques dirigidos ha generado un creciente número de soluciones. A fin de recopilar, almacenar y procesar los datos no estructurados generados, que permitan identificar y priorizar los ataques multinivel complejos, los procesos existentes deben actualizarse. Entre ellas:

- la jerarquización manual de amenazas y la evaluación de factores potencialmente indicativos de un posible ataque dirigido;
- la recopilación de información sobre ataques dirigidos y amenazas sobre estadísticas avanzadas;
- la identificación y la respuesta a incidentes;
- el análisis de objetos sospechosos en el tráfico de red y archivos adjuntos de correo electrónico;
- la detección de actividad inusual o anormal dentro de la infraestructura protegida

Las grandes empresas responden a las amenazas avanzadas actuales cambiando a una gestión centralizada de la seguridad de la información, consolidando los datos desde soluciones de seguridad dispares (mediante la recopilación automatizada y la correlación de eventos: SIEM) y unificando su presentación con la creación de centros de supervisión de seguridad (SOC, centro de operaciones de seguridad). Pero para que este enfoque resulte eficaz frente a los ataques dirigidos y las amenazas avanzadas, es preciso comprender a fondo los problemas de seguridad y el análisis de las ciberamenazas.

Solución Threat Management and Defense

Kaspersky Lab fue la primera empresa tecnológica que estableció un laboratorio de amenazas avanzadas en 2008.

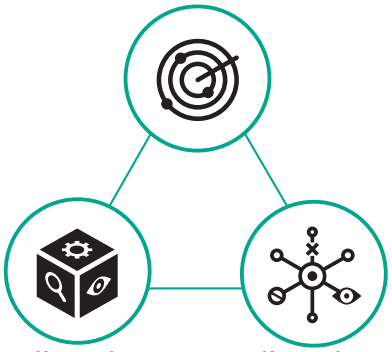
Así es cómo hemos descubierto más amenazas dirigidas y avanzadas que ningún otro proveedor de seguridad. Cuando en las noticias se informa de la última amenaza persistente avanzada, es probable que el equipo de élite global de investigación y análisis (GReAT) de Kaspersky Lab la detectara.

Con una envidiable trayectoria en la detección de ataques dirigidos y APT, nuestro equipo GReAT es famoso por su inteligencia sobre amenazas. El equipo ha jugado un papel decisivo en la detección de muchos de los ataques más sofisticados, entre los que se incluyen los siguientes:

- Stuxnet
- Octubre Rojo
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

...y muchos más.

Kaspersky Anti Targeted Attack: Protección frente a amenazas complejas



Kaspersky Cybersecurity Services: Información sobre seguridad o externalización

Kaspersky Endpoint Detection and Response: Visibilidad total

Los conocimientos de Kaspersky Lab sobre el funcionamiento interno de algunas de las amenazas más sofisticadas del mundo nos han permitido desarrollar una cartera de servicios y tecnologías de seguridad estratégicos capaces de ofrecer un enfoque totalmente integrado y adaptable en cuanto a la seguridad. Con nuestra experiencia, Kaspersky Lab ha conseguido más primeros puestos en pruebas independientes de detección y mitigación de amenazas que cualquier otra empresa de seguridad de IT. Hemos reunido esta competencia en la detección de ataques dirigidos en una solución independiente gracias a dos décadas de análisis e investigación de amenazas generando tecnologías probadas y maduras.

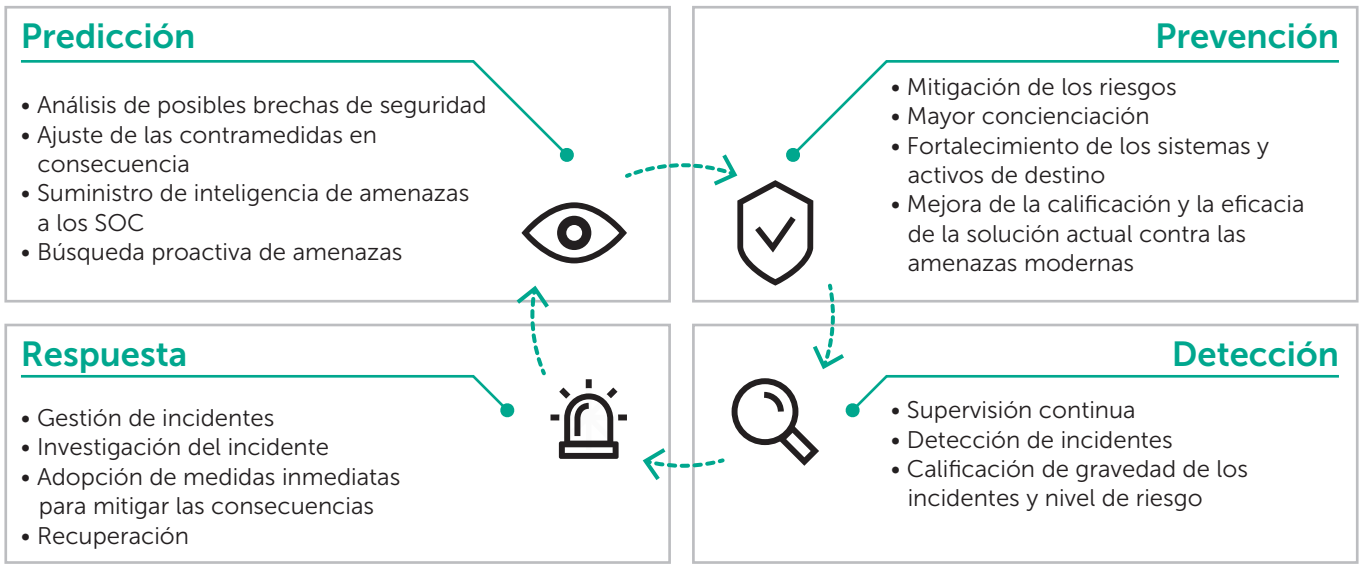
Si bien la mayoría de ciberamenazas simples puede bloquearse con productos de seguridad tradicionales basados en firma y mejorados con heurística, los hackers y cibercriminales de hoy día usan ataques cada vez más sofisticados dirigidos a organizaciones específicas. Los ataques dirigidos, incluidas las amenazas persistentes avanzadas (APT), se encuentran entre los riesgos más peligrosos a los que se enfrentan las empresas. No obstante, mientras que las amenazas, y las técnicas que los cibercriminales y hackers emplean, evolucionan constantemente, muchas empresas no acaban de adaptar sus estrategias de seguridad.

La combinación de detección a varios niveles de la plataforma Kaspersky Anti Targeted Attack y la rápida reacción de Kaspersky EDR con los servicios de inteligencia de ciberseguridad y asistencia premium permite a Kaspersky Threat Management and Defense proporcionar una solución unificada con administración centralizada, capaz de automatizar y facilitar todo el ciclo de gestión de amenazas avanzadas.

Difíciles de detectar y, a menudo, incluso más difíciles de eliminar, los ataques dirigidos y las amenazas avanzadas exigen una estrategia de seguridad adaptable y exhaustiva. La solución Kaspersky Threat Management and Defense se desarrolla a partir de la arquitectura de seguridad más viable, según lo describe Gartner. Nuestro enfoque es proporcionar un ciclo de actividades en cuatro áreas clave: prevención, detección, respuesta y predicción.

- **Prevención**: reduzca el riesgo de amenazas avanzadas y ataques dirigidos
- **Detección**: identifique actividades que podrían indicar un ataque dirigido
- **Respuesta**: colme las brechas de seguridad e investigue los ataques
- **Predicción**: sepa dónde y cómo podrían producirse nuevos ataques dirigidos

Básicamente, este enfoque da por supuesto que la prevención tradicional debería funcionar en coordinación con tecnologías de detección avanzadas, análisis de amenazas, capacidades de respuesta y técnicas de seguridad predictivas. Esto ayuda a crear un sistema de ciberseguridad que se adapta y responde continuamente a los desafíos empresariales emergentes.



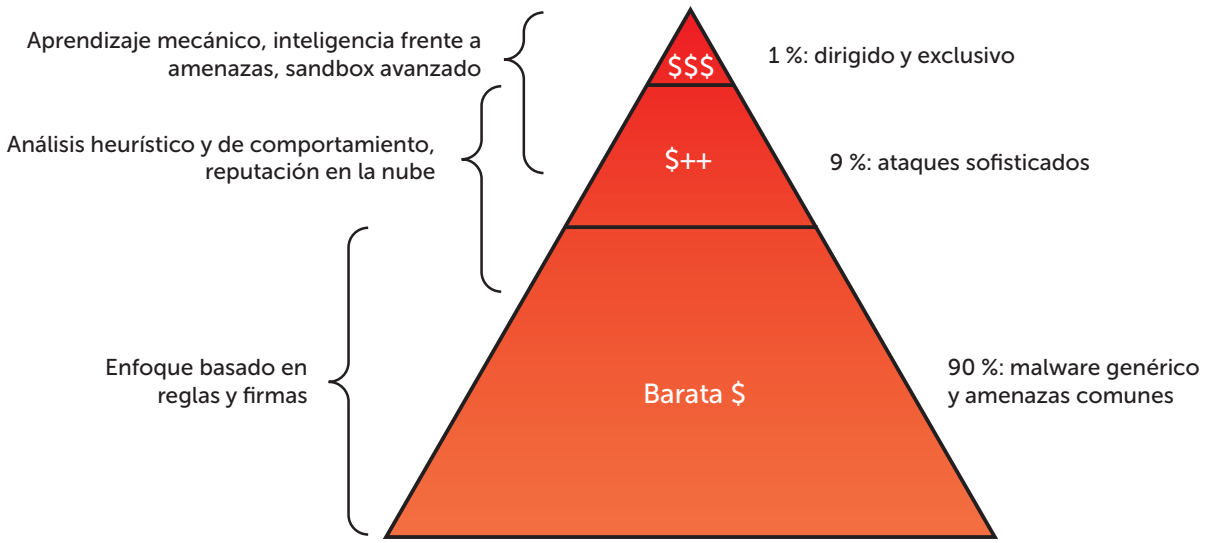
Prevención: uso de tecnologías de seguridad premiadas para disminuir el riesgo de ataques dirigidos

En el caso de los ataques dirigidos, las tecnologías de prevención son útiles para descartar los incidentes innecesarios, los objetos maliciosos comunes y las comunicaciones irrelevantes.

Pero también es importante reforzar todo el sistema con soluciones de seguridad específicas, así como educar sobre la seguridad e informar. Todo esto hará que los atacantes se vean obligados a dedicar más tiempo e inversiones si desean penetrar en su perímetro controlado y bien podría considerarle como una víctima demasiado costosa a la que dirigir sus ataques.

Los productos de seguridad basados en la prevención pueden ofrecer una protección muy eficaz frente a amenazas comunes, como el malware, los ataques de red y la filtración de datos. Pero incluso estas tecnologías no bastan en sí mismas para proteger a una empresa de los ataques dirigidos. Durante este tipo de ataques, las tecnologías de seguridad convencionales basadas en la prevención pueden detectar ciertos incidentes, pero suelen fallar a la hora de determinar si los incidentes aislados forman parte de un ataque mucho más complejo y peligroso que podría estar causando graves daños a su empresa y que seguirá infringiéndolos a largo plazo.

Sin embargo, las tecnologías basadas en la prevención a varios niveles siguen siendo un elemento fundamental de este nuevo enfoque proactivo para la protección contra ataques dirigidos.



Cómo abordar diferentes amenazas con tecnologías de seguridad

El 80 % de los ataques dirigidos empiezan con un correo electrónico malicioso que contiene un archivo adjunto o un enlace.

Entre los objetivos de ataque preferidos de los cibercriminales se incluyen RR. HH., los centros de llamada, los asistentes personales de los órganos de gestión directivos y las áreas externalizadas de la empresa. Estas funciones se identifican como las áreas menos preparadas de la organización

Es fundamental que las organizaciones sigan usando tecnología de seguridad "tradicional" para:

1. Filtrar y bloquear por medios automatizados eventos e incidentes no relacionados con los ataques dirigidos, lo que ayudará a evitar la asignación de personal a tareas innecesarias y centrar así la atención en la detección de incidentes importantes

2. Reforzar la infraestructura de IT frente a técnicas baratas y fáciles (ingeniería social, dispositivos extraíbles, dispositivos móviles, malware y propagación de malware por correo electrónico, etc.). En realidad, las inversiones anteriores para proteger el perímetro y los endpoints, junto con los controles implementados, dificulta a los cibercriminales el objetivo de penetrar en su red.

No obstante, si el atacante está suficientemente motivado y quizá incluso contratado por un tercero para llevar a cabo un ataque con éxito, un enfoque centrado exclusivamente en la prevención no bastará.

Detección de amenazas avanzadas por varios vectores antes de que el daño ocurra

La plataforma Kaspersky Anti Targeted Attack (KATA) incluye:

- **Arquitectura de sensores de varios niveles**, que aporta visibilidad total. KATA ofrece detección avanzada en cada nivel de su infraestructura de IT corporativa a través de una combinación de sensores de red, web y correo electrónico y endpoint.
- **Sandbox avanzado**, para evaluar nuevas amenazas. Nuestro sandbox avanzado es el resultado de más de una década de desarrollo continuo y ofrece un entorno virtualizado aislado para que los objetos sospechosos puedan ejecutarse de forma segura y sea posible observar su comportamiento.
- **Potentes motores de análisis**: para veredictos rápidos y menos falsos positivos.
  Nuestro analizador de ataques dirigidos evalúa los datos de los sensores de red y endpoints, y genera rápidamente veredictos de detección de amenazas para el equipo de seguridad.

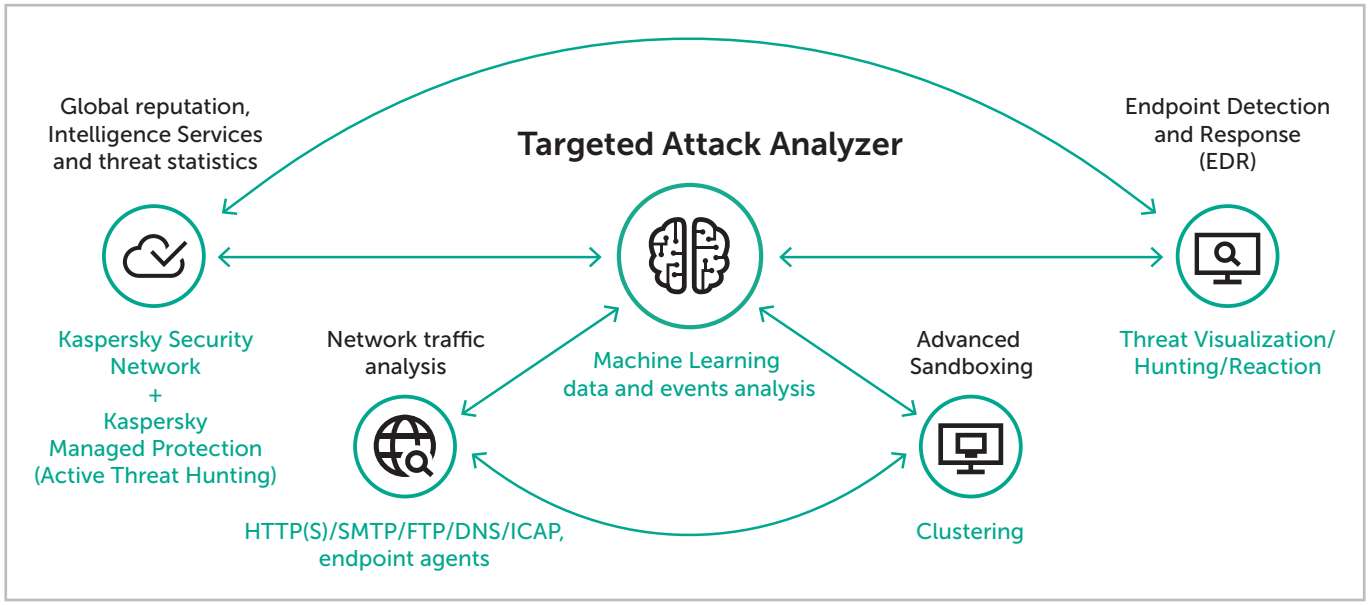
Cuanto antes se detecte un ataque, menores serán las pérdidas económicas y menores serán los procesos interrumpidos en su organización. Por tanto, la calidad y efectividad de la detección es crucial.

Los ataques dirigidos son compuestos y complejos, de modo que para detectarlos es necesario saber perfectamente cómo funcionan los ataques dirigidos y avanzados. Las soluciones antimalware simples no presentan defensa ante este tipo de ataques. En su defecto, necesita tecnologías de detección capaces de acceder a datos de inteligencia sobre amenazas actualizados y que realicen análisis detallados de posibles comportamientos sospechosos en distintos niveles de su red corporativa.

La capacidad de detectar ataques dirigidos comprende servicios y soluciones conectadas que puedan ofrecer:

- Formación
- **Experiencia en detección de ataques dirigidos**: auditoría de la infraestructura para localizar rastros de elementos cuya seguridad se haya visto comprometida
- **Solución especializada**: plataforma Kaspersky Anti Targeted Attack + Kaspersky Endpoint Detection and Response
- **Fuentes de datos de amenazas** para el intercambio de amenazas y actualizaciones sobre amenazas nuevas en tiempo real
- **Informes de APT y personalizados** para conocer mejor los métodos y las fuentes de amenazas
- **Búsqueda de amenazas 24/7** Kaspersky Managed Protection Service

La plataforma Kaspersky Anti Targeted Attack, basada en inteligencia de seguridad líder y tecnologías de aprendizaje mecánico avanzadas, combina datos de red y endpoint, sandbox y análisis inteligente para correlacionar los incidentes, buscar indicadores de compromiso y ayudar a detectar ataques dirigidos más complejos. La conexión de diversos rastros de un incidente proporciona una vista completa de toda la cadena de ataque, lo que aumenta la confianza en las puntuaciones de amenazas asignadas y reduce los falsos positivos a cero.

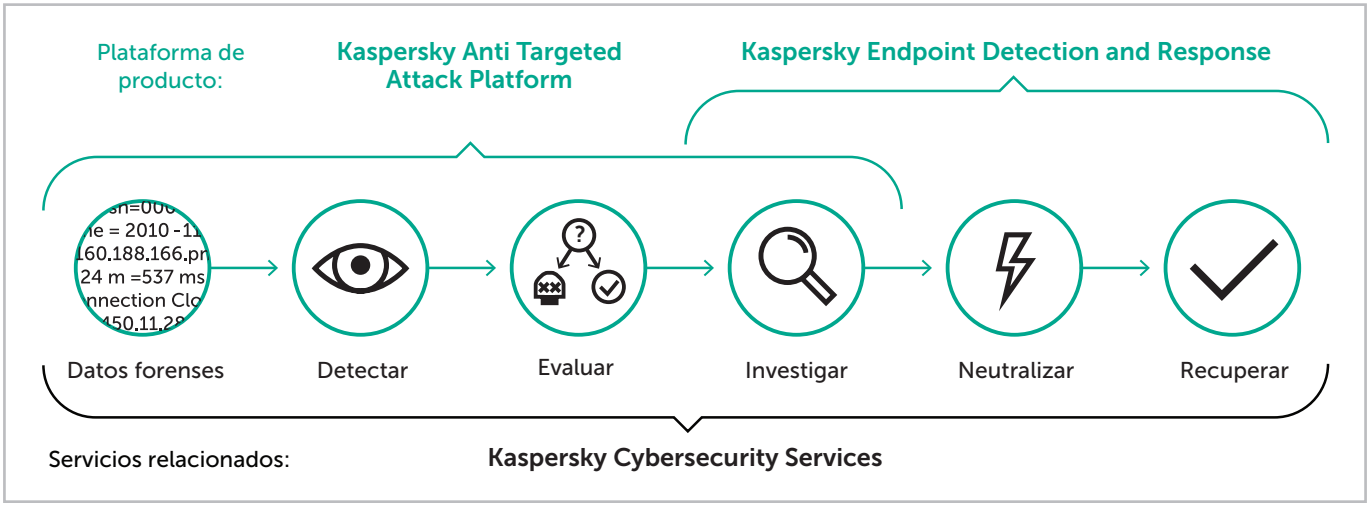


Respuesta: ayudar a las empresas a recuperarse de los ataques

Obviamente, lograr un mayor índice de detección solo es una parte de la batalla. Las mejores tecnologías de detección no sirven de nada si no tiene las herramientas y la experiencia necesarias para responder rápidamente a las amenazas "vivas" con potencial de causar daños en su organización.

Tras detectar un ataque, es importante disponer de acceso a expertos en seguridad reputados con competencias y experiencia para:

- Evaluar y rectificar el daño
- Recuperar rápidamente las operaciones.
- Obtener información tras la investigación de los incidentes sobre la que elaborar un plan de acción
- Planificar acciones para evitar que se repita el mismo escenario de ataque



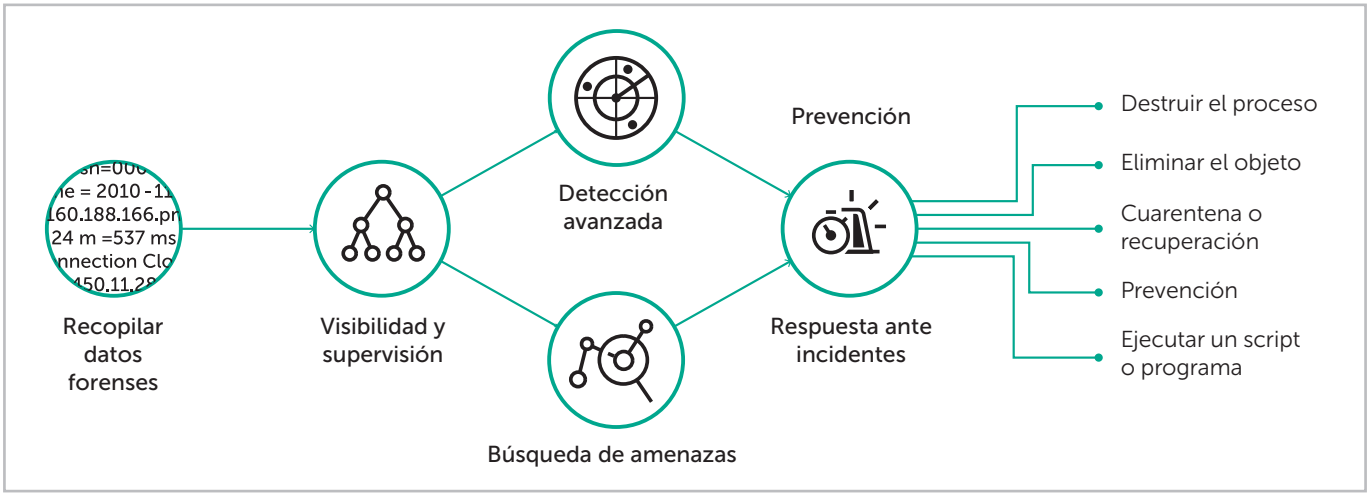
Kaspersky Endpoint Detection and Response ofrece:

- **Detección avanzada**: con el motor de aprendizaje mecánico Analizador de ataques dirigidos (TAA), que crea una referencia del comportamiento de los endpoints. Esto permite generar un registro histórico que se puede utilizar para descubrir cómo se ha producido una brecha.
- **Búsqueda de amenazas proactiva** con búsquedas rápidas en una base de datos centralizada, además de indicadores de compromiso (IoC) para ayudar al equipo de seguridad a buscar activamente las amenazas, análisis proactivo de endpoints para identificar anomalías y brechas de seguridad.
- **Respuesta adaptable a las amenazas**, que incluye una amplia gama de respuestas automatizadas que ayudan a las empresas a evitar el uso de procesos de corrección tradicionales (como el borrado de datos o la repetición de la generación de imágenes) que pueden tener como resultado un costoso tiempo de inactividad y la pérdida de productividad.

Cuando la plataforma Kaspersky Anti Targeted Attack de la solución de seguridad de un tercero identifica que su empresa está siendo atacada, el relevo pasa a Kaspersky Endpoint Detection and Response. Es el siguiente componente vital de la solución Threat Management and Defense, que permite a las empresas acelerar su proceso de respuesta a incidentes y mejorar la calidad de la investigación de los incidentes de ciberseguridad.

Kaspersky EDR proporciona una gestión centralizada de los incidentes en todos los endpoints de la red corporativa gracias a un flujo de trabajo perfecto e integración con la red a través de la plataforma Kaspersky Anti Targeted Attack. Una amplia variedad de respuestas automatizadas permite eliminar el costoso tiempo de inactividad y la pérdida de productividad inherentes a los procesos de corrección tradicionales, como el borrado de datos o la repetición de la generación de imágenes. La supervisión y el control de una amplia gama de funciones a través de una única interfaz permiten realizar las tareas de seguridad de manera más eficaz y eficiente, sin necesidad de alternar entre herramientas distintas y varias consolas.

La visibilidad total y una detección precisa son solo una parte de la batalla. La propia naturaleza de los ataques dirigidos implica que los atacantes volverán a intentarlo con nuevas técnicas y herramientas. En casos de emergencia, el equipo de ciberseguridad podría necesitar un socio de confianza con los conocimientos y la experiencia necesarios, así como el perfeccionamiento de las habilidades internas.



Nuestro servicio de respuesta a incidentes incluye:

- **Evaluación del incidente.** Análisis inicial de un incidente: se ejecuta rápidamente para minimizar el daño en su empresa (el análisis puede realizarse localmente o de forma remota)

- **Recopilación de pruebas.** Por ejemplo, recopilación de imágenes de la unidad de disco duro, volcados de memoria, rastros en la red y otra información pertinente del incidente

- **Análisis de ciencia forense.** Análisis detallado para aclarar información sobre:
  - Qué se ha atacado
  - Quiénes realizaron el ataque
  - Periodo durante el cual la empresa fue atacada
  - Dónde se originó el ataque
  - Por qué se atacó a su empresa
  - Cómo se ejecutó el ataque.

- **Análisis de malware.** Análisis detallado del malware utilizado como parte del ataque.

- **Plan de corrección.** Un plan detallado que ayudará a su empresa a prevenir la propagación de malware a través de la red, además de servirle para crear un plan de desinstalación.

- **Informe de investigación.** Un informe detallado con información sobre la investigación de los incidentes y su corrección.

Si su propio equipo de seguridad es capaz de realizar diversas tareas de respuesta a incidentes, quizá le interesa usar uno de nuestros otros servicios:

- **Servicio de análisis de malware**: somete a un análisis detallado el malware que su equipo ha aislado.

- **Servicio de análisis forense digital**: analiza las pruebas digitales y los efectos de los incidentes recopilados por su equipo.

Predicción: hacer más para protegerse frente a las amenazas futuras.

Dado el panorama de amenazas en constante cambio, su estrategia de seguridad debe evolucionar constantemente para hacer frente a los nuevos retos.

La seguridad no es una "actividad puntual", es un proceso constante que pasa por la evaluación continua de:

- Las últimas amenazas
- La eficacia de su estrategia de seguridad de IT

para que su empresa pueda adaptarse a los nuevos riesgos y las exigencias cambiantes.

Acceso a la inteligencia global de amenazas con Kaspersky Lab.

Disponer de acceso a expertos que sepan mantenerle al día en el panorama de amenazas global, y le ayuden a evaluar sus sistemas y defensas existentes es determinante para que su organización se adapte y conozca las nuevas amenazas de seguridad.

Con los años, nuestros expertos en seguridad globales han ido acumulando un dilatado conocimiento sobre el funcionamiento de los ataques dirigidos y avanzados, y analizamos constantemente nuevas técnicas de ataque. Esta experiencia ganada a pulso nos permite estar preparados para anticiparnos a los métodos de ataque nuevos y ayudarle a combatirlos.

Además, ofrecemos servicios especializados para que refuerce su infraestructura de IT:

- Servicios de Pen Testing para ayudarle a evaluar la eficacia de sus medios de seguridad actuales
- Servicios de evaluación de la seguridad de las aplicaciones: para ayudarle a detectar vulnerabilidades de software, antes de que lo hagan los cibercriminales
- Formación avanzada en ciberseguridad: para capacitar a sus propios expertos y permitirle crear su centro de operaciones de seguridad
- Informes de amenazas personalizados e informes de inteligencia: para mantenerle al tanto en el panorama de amenazas actual de constantes cambios
- Portal de búsqueda de amenazas: acceso a la base de datos mundial de inteligencia de Kaspersky Lab para facilitar sus investigaciones de malware

La estrategia de seguridad adaptable de Kaspersky desarrollada sobre la arquitectura de seguridad más viable descrita por Gartner. El enfoque de Kaspersky Lab comprende un ciclo de actividades en cuatro áreas clave: prevención, detección, respuesta y predicción. Básicamente, este enfoque da por supuesto que los sistemas de prevención tradicionales deberían funcionar en coordinación con tecnologías de detección, análisis de amenazas, capacidades de respuesta y técnicas de seguridad predictivas. Esto ayuda a crear un sistema de ciberseguridad que se adapta y responde continuamente a los desafíos empresariales emergentes.

La adopción de la solución Threat Management and Defense de Kaspersky Lab supone:

1. Pasar de un modelo de seguridad reactivo a un modelo proactivo basado en capacidades de gestión del riesgo, supervisión continua, respuesta más fundada a incidentes y búsqueda de amenazas.

2. Su marco operacional racionaliza los procesos de seguridad diarios y potencia la eficacia de la seguridad a través de un modelo de defensa de varios niveles que previene y detecta las amenazas avanzadas en cada fase del ataque.

3. Una plataforma integrada reduce las alertas que desbordan a la mayoría de equipos de seguridad, ya que proporciona un contexto basado en la inteligencia de amenazas y un sistema de jerarquización de alertas, así como una mejora de las respuestas tácticas gracias al uso compartido de conocimientos sobre amenazas y una amplia experiencia basada en la prestación de servicios de inteligencia de seguridad.

4. Este entorno ofrece a los analistas de seguridad visibilidad en todas las fases de los ataques de forma unificada, que favorece la integridad de los análisis de amenazas y la fiabilidad de las investigaciones de las amenazas conocidas y desconocidas antes de que afecten a la empresa.

5. Compartir la inteligencia sobre amenazas global mediante APT y portales específicos permite obtener perspectivas proactivas de los motivos e intenciones de sus adversarios, para que pueda priorizar las políticas y la planificación de las inversiones en seguridad de la forma correspondiente.

Las tecnologías de Kaspersky Lab acumulan un mundo de experiencia

La eficacia de los productos de Kaspersky Lab se demuestra de manera regular a través de pruebas independientes. En 2015, la empresa encabezó la lista de los tres principales fabricantes de soluciones de seguridad. Según los resultados de 84 pruebas diferentes realizadas por reputadas entidades de certificación en varios países, las soluciones de Kaspersky Lab acabaron entre las tres primeras en el 82 % de las pruebas y lideraron la clasificación en 60 ocasiones. Esta es una prueba innegable de que Kaspersky Lab ofrece la mejor protección del sector.

Solución probada contra amenazas avanzadas

Durante 2017, nuestra plataforma Kaspersky Anti-Targeted (como parte de la solución Threat Management and Defense) ha seguido participando en pruebas de ICSA Labs.

Las últimas pruebas duraron 37 días y consistieron en 585 ataques y 519 archivos limpios. KATA demostró excelentes resultados:

- Índice de detección perfecto: 100 % (cero muestras sin detectar)
- Menor índice de falsos positivos: 0 %
- Estado "Certificado" acreditado

Las siguientes son algunas citas del informe resultante publicado por ICSA el 7 de julio:

- "La solución de Kaspersky obtuvo resultados notables durante este ciclo de pruebas".
- "La plataforma KATA Kaspersky Lab detectó el 100 % de las amenazas durante las pruebas, un resultado considerablemente mejor que el porcentaje exigido para la certificación".
- "KATA de Kaspersky Lab hizo gala de una excelente eficacia en la detección de amenazas con casi 600 amenazas nuevas y poco conocidas".
- "Independientemente de si la amenaza era nueva o antigua, la plataforma KATA de Kaspersky detectó todas las amenazas maliciosas nuevas y poco conocidas".
- "La plataforma KATA de Kaspersky arrojó cero falsos positivos durante este ciclo de pruebas, un resultado sin duda excelente".
- "KATA, la solución de defensa contra amenazas avanzadas de Kaspersky Lab superó todos los casos de pruebas para obtener la certificación de defensa contra amenazas avanzadas de ICSA Labs. Es el tercer trimestre consecutivo en el que Kaspersky Lab completa este ciclo de pruebas con tan buenos resultados y supera los criterios para la certificación ATD de ICSA Labs".

NOTA: La metodología de pruebas de ICSA es dinámica y cambia cada trimestre. La prueba en sí simula con continuos cambios un entorno real y métodos de ataque. El nivel de seguridad no se mide en un momento dado, sino a largo de un periodo extenso (más de 30 días) de operaciones continuas bajo el acoso de numerosos ataques. De esta forma, la prueba pretende demostrar la eficiencia y eficacia de una solución desde la posición de un usuario.

Enfoque integral y visionario

Radicati Group lleva varios años realizando un análisis independiente del mercado de soluciones de protección APT para identificar los actores principales, los pioneros, los especialistas y los actores maduros. Entre los resultados del último análisis que acaba de publicarse se evaluó de forma excelente el enfoque de Kaspersky Lab para contrarrestar los ataques dirigidos y las amenazas avanzadas.

En 2017, la solución de Kaspersky mejoró significativamente su posición con un importante salto de especialista a líder pionero.

Los proveedores distinguidos como "pioneros" ofrecen tecnología avanzada en algunas áreas de sus soluciones, pero no necesariamente tienen todas las características y funcionalidad a partir de las que destacarían como actores principales. Sin embargo, los pioneros pueden revolucionar el mercado con nuevas tecnologías o nuevos modelos de servicios. Es muy probable que estos proveedores lleguen a ser actores principales.

"La plataforma Kaspersky Anti Targeted Attack proporciona detección de amenazas avanzadas y ataques dirigidos en todos los niveles de un ataque dirigido: infección inicial, comunicaciones de mando y control, movimientos laterales y exfiltración de datos".

Kaspersky Lab Iberia
Ciberseguridad de empresa: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.lat/**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.es